

03/03/00



Jc777 U.S. PTO

# UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. **US 008002** Total Pages 25

First Named Inventor or Application Identifier

**Fleming et al**

Express Mail Label No. EJ 903756252 US

Date of Deposit **3 March 3000**



## APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☒ **Fee Transmittal Form**  
(Submit an original, and a duplicate for fee processing)

2. ☒ **Specification** *Total Pages 15*  
(preferred arrangement set forth below)
- Descriptive title of the Invention
  - Cross References to Related Applications
  - Statement Regarding Fed sponsored R & D
  - Reference to Microfiche Appendix
  - Background of the Invention
  - Brief Summary of the Invention
  - Brief Description of the Drawings (if filed)
  - Detailed Description
  - Claim(s)
  - Abstract of the Disclosure

3. ☒ **Drawings (35 USC 113) Total Sheets 1**

4. ☒ **Oath or Declaration** *Total Pages 4*
- a. ☒ **Newly executed** (original or copy)
  - b. ☐ **Copy from a prior application**  
(37 CFR 1.63(d))

(for continuation/divisional with Box 17 completed)

[Note Box 5 below]

- i. ☐ **DELETION OF INVENTOR(S)**  
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. ☐ **Incorporation By Reference**  
(useable if Box 4b is checked)  
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ☐ **Microfiche Computer Program** (Appendix)
7. ☐ **Nucleotide and/or Amino Acid Sequence Submission**  
(if applicable, all necessary)
- a. ☐ **Computer Readable Copy**
  - b. ☐ **Paper Copy** (identical to computer copy)
  - c. ☐ **Statement verifying identity of above copies**

## ACCOMPANYING APPLICATION PARTS

8. ☒ **Assignment Papers** (cover sheet & document(s))
9. ☐ **37 CFR 3.73(b) Statement** ☐ **Power of Attorney**  
(when there is an assignee)
10. ☐ **English Translation Document** (if applicable)
11. ☐ **Information Disclosure Statement (IDS)/PTO 1449** ☐ **Copies of IDS Citations**
12. ☐ **Preliminary Amendment**
13. ☒ **Return Receipt Postcard (MPEP 503)**  
(Should be specifically itemized)
14. ☐ **Small Entity Statement(s)** ☐ **Statement filed in Prior Application, Status still proper and desired.**
15. ☐ **Certified Copy of Priority Document(s)**  
(if foreign priority is claimed)
16. ☒ **Other**  
☒ **Check in the amount of \$730**


17. If a **CONTINUING APPLICATION**, check appropriate box and supply the requisite information:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No:

18. **CORRESPONDENCE ADDRESS:** Corporate Patent Counsel  
U.S. Philips Corporation  
580 White Plains Road  
Tarrytown, N.Y. 10591

## 19. Certificate of Express Mail:

I hereby certify that this paper and the items identified above are being deposited with the U.S. Postal Service "Express Mail Post Office to Addresses" service under 37 C.F.R. Section 1.10 on the 'Date of Deposit', indicated above, and is addressed to: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

  
Robert M. McDermott, Registration Number 41,508

## BACKGROUND OF THE INVENTION

### 1. Field of the Invention

5 This invention relates to the field of communications, and in particular to secure communications via an IEEE 1394 (firewire) interface.

### 2. Description of Related Art

Secure communications between and among devices is becoming increasingly important  
10 for the protection of copyright material and other communiqués. An organization known as the Digital Transmission Licensing Authority (DTLA) has created the Digital Transmission Content Protection Specification, commonly known as the "5C" specification. The 5C specification defines a cryptographic system comprising a number of cryptographic components, including methods for enciphering and deciphering content material, and methods for determining secure cryptographic  
15 keys for use in this enciphering and deciphering of the content material.

A commonly used protocol for the transmission of audio/visual material among audio/visual applications is the IEEE 1394 protocol and interface. Special purpose controllers have been developed to support the transfer of enciphered material between an application program and the IEEE 1394 bus interface, including the enciphering and deciphering of the  
20 content material being transferred in accordance with the 5C specification, based on cryptographic keys that are provided by the application program. As is known in the art, given a sufficiently robust key, the enciphering and deciphering of information can provide a high level of security, and can be effected with relatively little overhead, being based primarily on a "shift and add" or similar operation. The complexity required to generate the keys that are used to perform the  
25 enciphering and deciphering, on the other hand, is substantial. To minimize the potential damage caused by a breach of security of keys, the 5C specification calls for the generation of unique keys by the devices involved in the transfer of the information. A discovery of the keys that are used by one pair of devices provides no information concerning the keys used by another pair of devices. When a communication of protected information is required, the devices generate a unique set of  
30 keys for ciphering and deciphering the information. The generation of unique keys for each

session of information transfer is effected via a "key exchange", which is an exchange of parameters that are used to generate keys within each device.

In the 5C specification, an elliptic curve Diffie-Hellman key exchange, and an elliptic curve Digital Signature algorithm is specified for full authentication. The elliptic curve computations are known in the art, and are mathematically complex. For sufficient security, the computations use relatively large numbers, in the order of 160 or more bits. The 5C specification requires that these operations be completed in a limited amount of time, for operation effectiveness, as well as security reasons. Because of the mathematical complexity and required efficiency, a conventional implementation of these tasks includes a software program that is executed on a high-performance microprocessor. For example, on a home computer system with an IEEE 1394 interface, the application program that is used to transfer the information to other devices contains the sub-programs that compute or verify digital signatures, and, if the signatures are verified, effect a key exchange. These sub-programs are typically run on a Pentium® or similar high performance processor, via, for example, a "C" program that includes complex operations that are known to be computationally irreversible. That is, a knowledge of the output of the complex operation provides little or no information regarding the parameters that were used to generate the output. For example, in the context of the 5C specification, elliptic curve cryptography is based on a determination of a point on an elliptic curve based on another point on the curve.

As the name "key exchange" implies, both the device that will be transmitting the protected information, and the device that will be receiving the protected information must participate in this exchange, and therefore both devices must contain sufficient capabilities to effect the above described key exchange computations. Although the execution of a key exchange on a home computer is feasible, the cost of a high performance microprocessor can be prohibitive in many applications, specifically consumer electronic equipment, such as video recorders, CD players, and the like. Additionally, each application program on a computer, and each component device that is expected to comply with the 5C specification, must incur the cost of developing and testing, or purchasing and testing, the software required to effect the digital signing and key exchange tasks required by the 5C specification. As an alternative to a high-performance processor running a software program, a special purpose processor can be provided to facilitate the 5C authentication functions, but such a special purpose processor can be expected to require a

substantial modification to existing processing systems designs and architectures, and will add costs to each device that is expected to comply with the 5C specification.

#### BRIEF SUMMARY OF THE INVENTION

5 It is an object of this invention to facilitate the task of 5C authentication and key exchange. It is a further object of this invention to facilitate the task of 5C authentication and key exchange in an IEEE 1394 environment. It is a further object of this invention to minimize the burden on application programs for effecting authentication and key exchange. It is a further object of this invention to minimize the cost of implementing 5C authentication and key exchange  
10 in an IEEE 1394 environment. It is a further object of this invention to provide a device that facilitates 5C authentication and key exchange in existing system architectures.

These objects and others are achieved by incorporating authentication and key exchange functions, such as those conforming to the Digital Transmission Licensing Authority's (DTLA) Digital Transmission Content Protection (5C) Specification, into a link-layer access device of a  
15 conventional processing system. Because of the suitability of IEEE 1394 for transferring audio/video information, these functions are preferably embodied in an IEEE 1394 compatible link-layer access device. The link-layer access device of this invention is configured to support, for example, the elliptic curve multiplication functions of a Diffie-Hellman key exchange process, as well as digital signature generation and digital signature verification. By incorporating the authentication and key exchange functions into a link-layer access device, the system architecture  
20 and devices that are commonly used in conventional processing systems can be used, thereby providing an incremental path toward increased protection of copyright material. In a preferred embodiment, the conventional link-layer controller is configured to implement the authentication and key exchange processes, via calls to the link-layer access device to perform the complex  
25 mathematical operations, thereby eliminating the need for each application-layer program or device to implement these processes.

## BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG. 1 illustrates an example block diagram of a processing system in accordance with this invention.

FIG. 2 illustrates an example block diagram of a link-layer access device that facilitates cryptographic authentication and key exchange functions, including key exchange functions, in accordance with this invention.

Throughout the drawings, the same reference numerals indicate similar or corresponding features or functions.

## DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates an example block diagram of a processing system 100 in accordance with this invention. By intent, the architecture of the processing system 100 is substantially identical to that of conventional prior-art processing systems. The processing system 100 includes an application device 110 that communicates with another device (not shown) via a physical-layer communications path, such as an IEEE 1394 bus 150. Consistent with common hierarchical protocol structures, the application device 110 transfers information to the physical-layer communications path via a link-layer access device 200 and a physical-layer access device 130. A node controller 120 manages the flow of information between the application device 110 and the link-layer access device 200, and the processing of information at the link-layer access device 200.

In accordance with this invention, the link-layer access device 200 includes an authentication and key exchange accelerator 250, as illustrated in FIG. 2. The authentication and key exchange accelerator 250 facilitates cryptographic tasks, such as key exchange, digital signing, and digital signature verification. Copending U.S. patent application, "Simple Algorithmic Cryptography Engine", U.S. serial number 09/466,392, filed 17 December 1999 for George Fleming, Farrell Ostler, and Antoine Dagher, provides a processing architecture that is particularly well suited for cryptographic processing, and is incorporated by reference herein. In the copending application, a variety of techniques are employed to minimize the complexity of the design and to minimize the complexity of the interconnections within the device, thereby allowing

the engine to be incorporated within an existing link-layer access device integrated circuit design. A variety of techniques are also employed to ease the task of programming the processor for cryptographic processes, and to optimize the efficiency of instructions that are expected to be required for effecting digital signing, verification, and key exchange. Because authentication and  
5 key exchange tasks are characterized by operations on wide data items, particular emphasis is placed on the efficient processing of multi-word operations, including the use of constants having the same width as an instruction word. A simplified arithmetic unit is provided that is specifically designed to support digital signing, verification and key exchange, with minimal overhead.

In a preferred embodiment of this invention, the link-layer access device 200 receives  
10 commands from the node controller 120 to effect the provided authentication and key exchange tasks. As is common in the art, the controller 120 is typically a low-cost microprocessor, such as an 8051-type controller, with insufficient processing power to provide the authentication and key exchange tasks. By providing the authentication and key exchange accelerator 250 in the link-layer access device 200, to which the node controller 120 is traditionally coupled, the  
15 authentication and key exchange tasks can be off-loaded from the application device 110 without introducing a change to the traditional processing system architecture. Preferably, the link-layer access device 200 of this invention has the same pin-out of prior art link-layer access devices, so that existing processing system designs can be upgraded to include authentication and key exchange capabilities via changes to the software and/or firmware used in the node controller 120.  
20 The resultant combination of node controller 120 and link-layer access device 200 substantially eliminates the need for application devices 110, and corresponding application-layer programs, to include the complex operations required to effect digital signing, verification, and key exchange, thereby minimizing the development time and cost for introducing DTLA 5C security to copy protected material.

25 The node controller 120 is configured to control the sequences involved in authentication and key exchange processes, and to provide cryptographic parameters and commands to the link-layer access device 200, as required, via the controller interface 220 of the link-layer access device 200. The authentication and key exchange accelerator 250 of the link-layer access device 200 is configured to perform the complex mathematical operations required to produce cryptographic  
30 items to fulfill each command, based on the parameters provided by the controller 120 or stored

within the link-layer access device 200. For ease of reference, the terms cryptographic items and parameters are used herein to include the parameters, arguments, intermediate results, final results, and so on, that are communicated among and between devices for the purpose of effecting a task related to cryptography, such as digital signing, verification, and key exchange and generation. In a preferred embodiment, the link-layer access device 200 is configured to perform the following operations, in response to corresponding commands from the node controller 120:

Basepoint Multiply (first phase of Diffie-Hellman key exchange)  
Point Multiply (final phase of Diffie-Hellman key exchange)  
EC-DSA Verify (verify digital signature of a message)  
EC-DSA Sign (digitally sign a message),

where EC-DSA corresponds to the Elliptic-Curve Digital Signature Algorithm, common in the art. The basepoint multiply and point multiply operations include the aforementioned elliptic curve multiplication operations that provide a point on an elliptic curve based on another point on the curve and one or more parameters associated with the elliptic curve Diffie-Hellman key exchange algorithm, common in the art. The EC-DSA verify operation verifies a source of a message from another device, based on a key associated with the other device. The EC-DSA sign operation binds a cryptographic item to the message, to facilitate a subsequent verification of the source of the message at another device, based on a key associated with this device.

In a Diffie-Hellman key exchange, each device chooses a local parameter, such as a large random number, and computes a particular function with this parameter as an argument. The result of this function is communicated to the other device. Each device then computes a second function with the communicated item and its local parameter as arguments. The two functions that are applied in this exchange are such that the result provided by the second function in each device is identical, and also such that knowledge of the communicated items provides no assistance to a third party in determining the common result. For example, consider  $x$  and  $y$  being the local parameters of each device, and the result of a modular exponentiation of a commonly known integer  $g$  by the local parameter  $x$ ,  $y$  ( $X = g^x \bmod m$ ;  $Y = g^y \bmod m$ ) being the communicated items  $X$  and  $Y$ , where  $m$  is also commonly known to each device. Each device computes a second modular exponentiation of the received item ( $K1 = Y^x \bmod m$ ;  $K2 = X^y \bmod m$ ). Both  $K1$  and  $K2$  will be equal to  $g^{xy} \bmod m$  ( $K1 = (g^y \bmod m)^x \bmod m$ ;  $K2 = (g^x \bmod m)^y$

mod  $m$ ), and, provided that  $x$ , and  $y$  are large, a knowledge of  $g$ ,  $m$ ,  $X$ , and  $Y$  provides little or no assistance in determining the value  $g^{xy} \bmod m$ . This common result of the second function ( $g^{xy} \bmod m$ ) at each device is used as the key for ciphering and deciphering messages. In an embodiment that satisfies the 5C specification, the functions are elliptic curve functions, rather than exponentiation functions, although this invention is not, per se, limited to the 5C specification or elliptic curve functions. In a preferred embodiment, the link-layer access device 200 facilitates the authentication processes of signing and verifying, as well as key exchange, by providing operations that are commonly used in cryptographic applications, such as exponentiation or elliptic curve multiplications, and are too complex for embodiment in a low-cost microcontroller 120. The microcontroller 120 in this preferred embodiment, on the other hand, controls the sequence of operations, the communication of parameters with the link-layer access device 200, and so on, to effect the appropriate authentication and key exchange tasks.

The link-layer access device 200 of this invention includes the components required to perform conventional link-layer access operations, thereby providing the aforementioned authentication and key exchange operations at a minimal incremental cost compared to conventional processing system. The link-layer access device 200 includes an application-layer interface 210 that provides the communications interface with the application device, or devices, 110 of FIG. 1, and a physical-layer interface 230 that provides the communications interface with the physical-layer device, or devices, 130. Conventional control and status registers 260 are used to facilitate the interaction of the link-layer access device 200 with the physical and application layer devices via the appropriate interface 230, 210. For example, the 1394 protocol supports both isochronous and asynchronous communications. The isochronous, or "real-time", data must be placed on, and removed from, the 1394 bus 150 at specific intervals, to achieve, for example video renderings at a specific frame rate. Asynchronous communications are achieved by communicating data whenever the bus 150 is available. The transmit/receiver buffer 240, as its name implies, buffers the data received from either domain, as required. As shown, for completeness, the link-layer access device 200 may include an optional cipher/decipher device 245 that ciphers or deciphers the information being transferred through the buffer 240. The key that is used for this cipher/decipher operation is provided to the device 245 by the node controller 120, via the controller interface 220, after the aforementioned key exchange process is completed.



The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within its spirit and scope. For example, the invention has been presented using the paradigm of DTLA 5C authentication and key exchange tasks in an IEEE 1394 environment. Although the details of this invention are particularly well suited for DTLA 5C authentication and key exchange and IEEE 1394 communications, one of ordinary skill in the art will recognize the suitability of this invention to other security schemes, and other communications protocols. In like manner, the authentication and key exchange accelerator 250 has been presented as supporting four operations that facilitate cryptographic operations, although fewer or more operations may be supported, depending upon the circuit area in the link-layer access device 200 that can be devoted to cryptographic tasks. For example, random number generation, hashing, and the like can be added to the link-layer access device 200, if the required circuit area for these functions is available. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.

## CLAIMS

We claim:

1. A processing system comprising:

an application device that is configured to communicate information with a physical-layer  
5 access device via a link-layer access device,

a node controller that is configured to control the link-layer access device,  
the link-layer access device, operably coupled to the application device, the node  
controller, and the physical-layer access device, that is configured to facilitate an exchange of the  
information from and to the application device with data that is communicated to and from the  
10 physical-layer access device;

wherein,

the link-layer access device is further configured to provide, in response to one or more  
commands from the node controller, one or more cryptographic items based on one or more  
parameters from the node controller.

2. The processing system of claim 1, wherein

the one or more cryptographic items include at least one of:

- a digital signature,
- a verification of a digital signature, and
- 20 a cryptographic key item.

3. The processing system of claim 1, wherein

the one or more cryptographic items include:

- a digital signature,
- 25 a verification of a digital signature, and
- a cryptographic key item.

4. The processing system of claim 1, wherein

the link-layer access device includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

5

5. The processing system of claim 1, wherein

the node controller is configured to effect an exchange of a cryptographic key with an other processing system, and

the one or more cryptographic items from the link-layer access device includes the  
10 cryptographic key.

6. The processing system of claim 1, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.

15

7. A link-layer access device comprising:

an application-layer interface device that is configured to communicate information with an application-layer device,

a physical-layer interface device that is configured to communicate data with a physical-layer device,

a buffer device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate an exchange of the information of the application-layer device and the data of the physical-layer device,

a controller interface device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate control of the exchange of information and data, and

an accelerator, operably coupled to a controller via the controller interface device, that is configured to compute one or more cryptographic items, in response to one or more cryptographic commands from the controller, and to thereafter communicate the one or more cryptographic items to the controller.

8. The link-layer access device of claim 7, wherein

the accelerator includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on one or more of parameters provided by the controller.

9. The link-layer access device of claim 7, wherein

the one or more cryptographic items includes at least one of:

a signature of a message,

a verification of a digital signature,

a hash of one or more parameters,

a random number,

an exponentiation of one or more parameters, and

an elliptic curve multiplication of one or more parameters,

the one or more parameters being provided by the controller.

10. The link-layer access device of claim 7, wherein  
the one or more cryptographic items include:

- 5           a signature of a message,  
          a verification of a digital signature, and  
          an elliptic curve multiplication of one or more parameters,  
the one or more parameters being provided by the controller.

11. The link-layer access device of claim 7, wherein

- 10       the one or more cryptographic commands include: a basepoint multiply command, a point  
multiply command, an EC-DSA Verify command, and an EC-DSA sign command.

11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206

12. A method for communications comprising:

communicating information from and to an application device to and from a physical-layer access device via a link-layer access device,

5 controlling the link-layer access device, in dependence upon commands from a node controller,

effecting an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device, and

determining one or more cryptographic items via computations within the link-layer access device, based on one or more parameters that are provided to the link-layer access device by the  
10 node controller.

13. The method of claim 12, wherein

the one or more cryptographic items include at least one of:

a digital signature,

15 a verification of a digital signature, and

a cryptographic key item.

14. The method of claim 12, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

15. The method of claim 12, wherein  
determining the one or more cryptographic items includes  
deriving a second point on an elliptic curve from a first point on the elliptic curve,  
based on the one or more of the parameters from the node controller.

5

15. The method of claim 12, further including  
effecting an exchange of a cryptographic key with an other processing system, wherein  
the one or more cryptographic items from the link-layer access device includes the  
cryptographic key.

10

16. The method of claim 12, wherein  
the commands from the node controller include: a basepoint multiply command, a point  
multiply command, an EC-DSA verify command, and an EC-DSA sign command.

15

ABSTRACT OF THE DISCLOSURE

Authentication and key exchange functions, such as those conforming to the Digital  
5 Transmission Licensing Authority's (DTLA) Digital Transmission Content Protection (5C)  
Specification, are incorporated into a link-layer access device of a conventional processing  
system. Because of the suitability of IEEE 1394 for transferring audio/video information, these  
functions are preferably embodied in an IEEE 1394 compatible link-layer access device. The link-  
layer access device of this invention is configured to support, for example, the elliptic curve  
10 multiplication functions of a Diffie-Hellman key exchange process, as well as digital signature  
generation and digital signature verification. By incorporating the authentication and key  
exchange functions into a link-layer access device, the system architecture and devices that are  
commonly used in conventional processing systems can be used, thereby providing an incremental  
path toward increased protection of copyright material. In a preferred embodiment, the  
15 conventional link-layer controller is configured to implement the authentication and key exchange  
processes, via calls to the link-layer access device to perform the complex mathematical  
operations, thereby eliminating the need for each application-layer program or device to  
implement these processes.



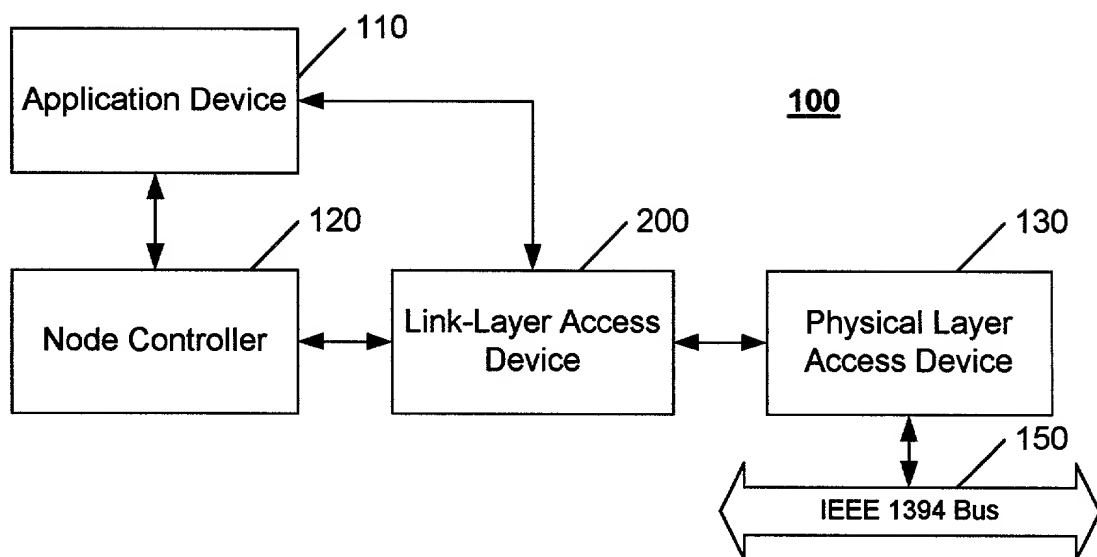


FIG. 1

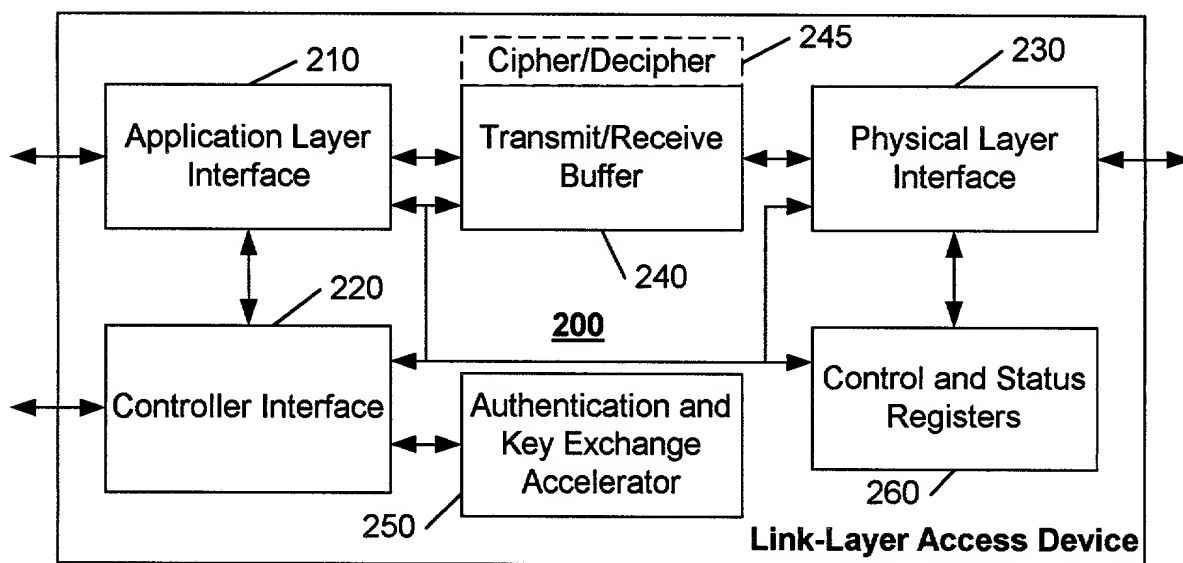


FIG. 2

**DECLARATION and POWER OF ATTORNEY**Attorney's Docket No. **US 008002**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **IEEE 1394 LINK LAYER CHIP WITH "5C" AUTHENTICATION AND KEY EXCHANGE ACCELERATOR** the specification of which (check one)

☒ is attached hereto.

was filed on as Application Serial No. \_\_\_\_\_ and was amended on \_\_\_\_\_ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by the amendment(s) referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulation, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

**PRIOR FOREIGN APPLICATION(S)**

COUNTRY	APPLICATION NUMBER	DATE OF FILING (DAY, MONTH, YEAR)	PRIORITY CLAIMED UNDER 35 U.S.C. 119

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application (s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

**PRIOR UNITED STATES APPLICATION(S)**

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (PATENTED, PENDING, ABANDONED)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**POWER OF ATTORNEY:** As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Algy Tamoshunas, Reg. No. 27,677

Jack E. Haken, Reg. No. 26,902

**SEND CORRESPONDENCE TO:**Corporate Patent Counsel;  
U.S. Philips Corporation; 580 White Plains Road; Tarrytown, NY 10591**DIRECT TELEPHONE CALLS TO:**Robert J. Kraus, Reg. 26,358  
(914) 333-9634

Dated: <b>2nd March 2000</b>		Inventor's Signature: <i>GF Fleming</i>	
Full Name of Inventor	Last Name <b>Fleming</b>	First Name <b>George</b>	Middle Name
Residence & Citizenship	City <b>Hampshire</b>	State or Foreign Country <b>United Kingdom</b>	Country of Citizenship <b>U.K.</b>
Post Office	Street <b>Oak Cottage, Slab Lane</b>	City <b>Hampshire</b>	State or Country Zip Code

s:\kr\Catalog2

Address	West Wellow Romsey		U.K.	SO51 6BY
---------	-----------------------	--	------	-------------

Dated: 2nd MARCH 2000		Inventor's Signature: Bruce Murray		
Full Name of Inventor	Last Name Murray	First Name Bruce	Middle Name	
Residence & Citizenship	City Hampshire	State or Foreign Country United Kingdom	Country of Citizenship U.K.	
Post Office Address	Street 12 Noyce Drive Fair Oak Eastleigh	City Hampshire	State or Country U.K.	Zip Code SO50 7LT

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name Tolsch	First Name Don	Middle Name	
Residence & Citizenship	City Albuquerque	State or Foreign Country NM	Country of Citizenship U.S.	
Post Office Address	Street 5836 Lost Dutchman NE	City Albuquerque	State or Country U.S.A.	Zip Code 87111

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name	First Name	Middle Name	
Residence & Citizenship	City	State or Foreign Country	Country of Citizenship	
Post Office Address	Street	City	State or Country	Zip Code

**DECLARATION and POWER OF ATTORNEY**Attorney's Docket No. **US 008002**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **IEEE 1394 LINK LAYER CHIP WITH "5C" AUTHENTICATION AND KEY EXCHANGE ACCELERATOR** the specification of which (check one)

☒ is attached hereto.☐ was filed on as Application Serial No. \_\_\_\_\_ and was amended on \_\_\_\_\_ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by the amendment(s) referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulation, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

**PRIOR FOREIGN APPLICATION(S)**

COUNTRY	APPLICATION NUMBER	DATE OF FILING (DAY, MONTH, YEAR)	PRIORITY CLAIMED UNDER 35 U.S.C. 119

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application (s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

**PRIOR UNITED STATES APPLICATION(S)**

APPLICATION SERIAL NUMBER	FILING DATE	STATUS (PATENTED, PENDING, ABANDONED)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**POWER OF ATTORNEY:** As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

Algy Tamoshunas, Reg. No. 27,677

Jack E. Haken, Reg. No. 26,902

<b>SEND CORRESPONDENCE TO:</b> Corporate Patent Counsel; U.S. Philips Corporation; 580 White Plains Road; Tarrytown, NY 10591	<b>DIRECT TELEPHONE CALLS TO:</b> Robert J. Kraus, Reg. 26,358 (914) 333-9634
---	---

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name <b>Fleming</b>	First Name <b>George</b>	Middle Name	
Residence & Citizenship	City <b>Hampshire</b>	State or Foreign Country <b>United Kingdom</b>	Country of Citizenship <b>U.K.</b>	
Post Office Address	Street <b>Oak Cottage, Slab Lane West Wello Romsey</b>	City <b>Hampshire</b>	State or Country <b>U.K.</b>	Zip Code <b>SO51 6BY</b>

s:\kr\Catalog2

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name <b>Murray</b>	First Name <b>Bruce</b>	Middle Name	
Residence & Citizenship	City <b>Hampshire</b>	State or Foreign Country <b>United Kingdom</b>	Country of Citizenship <b>U.K.</b>	
Post Office Address	Street <b>12 Noyce Drive Fair Oak Eastleigh</b>	City <b>Hampshire</b>	State or Country <b>U.K.</b>	Zip Code <b>SO50 7LT</b>

Dated: <b>3/2/00</b>		Inventor's Signature: <i>K. Tolisch</i>		
Full Name of Inventor	Last Name <b>Tolisch</b>	First Name <b>Don</b>	Middle Name	
Residence & Citizenship	City <b>Albuquerque</b>	State or Foreign Country <b>NM</b>	Country of Citizenship <b>U.S.</b>	
Post Office Address	Street <b>5836 Lost Dutchman NE</b>	City <b>Albuquerque</b>	State or Country <b>U.S.A.</b>	Zip Code <b>87111</b>

Dated:		Inventor's Signature:		
Full Name of Inventor	Last Name	First Name	Middle Name	
Residence & Citizenship	City	State or Foreign Country	Country of Citizenship	
Post Office Address	Street	City	State or Country	Zip Code